특정 IP 영역 제한정책 설정에 따른 보안 취약점 공격에 관한 연구

서우석* · 전문석**

A Study on Security Hole Attack According to the Establishment of Policies to Limit Particular IP Area

Woo-seok Seo* · Moon-seog Jun**

요 약

다양한 정보보안 구축 사례를 보면, Firewall과 가상 사설 통신망[VPN(Virtual Private Network)], 침입 탐지 시스템[IDS(Intrusion Detection System)], 기업 보안 관리[ESM(Enterprise Security Management)] 등 단계적인 발전 절차를 갖는다. 각각의 보안 솔루션과 장비는 특성화된 보안 기술을 통해서 TCP/IP Layer별 또는 공격형태, 공격유형, 침해로 인한 보안정책의 문제점과 같은 분류를 기준으로 정보보안 을 위한 방어와 공격을 분석한다. 본 논문의 연구 방향은 TCP/IP Layer의 L3 계층 이상의 상위 등급 보안정책과 장비를 통한 기존 네트워크에 L2 계층 이하 등급의 장비 또는 정책을 적용 시에 발생하는 침입 가능한 대기시간[Latency Time]을 확인하고 보안장비 정책에서 특정 IP 영역에 대한 제한정책 설정과정에서 IP 선점(Preoccupation)으로 인한 발생 가능한 보안 취약점을 분석함으로써 기술적인 문제점을 알아보고자 한다.

ABSTRACT

With regard to the examples of establishing various sorts of information security, it can be seen that there are gradual, developmental procedures including Firewall and VPN (Virtual Private Network), IDS (Intrusion Detection System), or ESM (Enterprise Security Management). Each of the security solutions and equipments analyzes both defense and attack for information security with the criteria of classifying the problems of security policies by TCP/IP layers or resulted from attack patterns, attack types, or invasion through specialized security technology. The direction of this study is to examine latency time vulnerable to invasion which occurs when L2-stratum or lower grade equipments or policies are applied to the existing network through TCP/IP layer's L3-stratum or higher grade security policies or equipments and analyze security holes which may generate due to the IP preoccupation in the process of establishing policies to limit particular IP area regarding the policies for security equipments to figure out technological problems lying in it.

키워드

Firewall, Switching, Preoccupation, Security Policy, DMZ(De-Militarized Zone)

* 숭실대학교 컴퓨터학과(ssws2003@yahoo.co.kr)
** 교신저자 : 숭실대학교 컴퓨터학과(mjun@ssu.ac.kr)
접수일자 : 2010. 10. 10
심사(수정)일자 : 2010. 11. 13
게재확정일자 : 2010. 12. 10

Ⅰ. 서 론

21세기 보안시장은 보안을 위한 또 다른 보안 정책을 도입하는 다단계적 솔루션을 구현한다. 기존의 정보보안 솔루션과 장비를 지속적으로 구현하면서 추가적인 솔루션 적용을 통해서 공격 목적과 공격 대상에 대한 분리를 통해 단계적으로 방어를 한다. 가장 흔히 쓰이고 있는 TCP/IP Layer 기반의 네트워크상에서 이루어지는 공격과 방어를 기준으로 수많은 정책과 장비가 운영된다. 또한, 반복적이고 지속적인 공격 패턴의 변화와 공격 패턴을 학습함으로써 방어기법과 정책을 설정하는 인공지능적인 분야로 확대되어 가고 있다. 그러나 과거 사용하던 보안 솔루션과 장비를 활용하면서 새로운 네트워크 인프라를 구현할 때 대부분의 구현에 있어서 L2 계층의 장비는 L3 계층 이상의 상위 등급 장비를 연결하는 부문에 운영된다. 이때 발생되는 장비간의 정책설정 반영을 위한 대기시간[Latency Time]이 발생함으로써 보안 취약점이 발생한다. 명확하게 공격의 대상이 되는 취약점이 발생하기보다는 L3 계층 이상의 장비와 L2 계층의 하위 등급의 장비 사이에서 정보보안 장비 간에 특정 IP 영역을 설정 시 IP 선점[Preoccupation]으로 Latency Time이 느려지는 장애가 발생하고 있다. 따라서 본 논문에서는 네트워크 구성 인프라 장비 중 Switching 기능을 탑재한 L2 계층의 장비로 인한 IP 선점 문제와 동일 계층의 보안 장비 사이에서 특정 IP 영역을 상호 정책 적용시의 보안 취약점을 연구하였다. 본 논문의 구성은 2장에서는 네트워크 인프라 구성을 통한 Switching과 IP선점 변화를 통한 문제를 제시하고, 3장에서는 다양한 정보보안 장비들의 특정 IP영역 정책설정 산의 취약점이 기술되고, 4장에서는 향후연구 방향과 결론을 기술했다.

Ⅱ. 네트워크 인프라 구성과 변화

네트워크에서 L2 및 L3 계층의 장비가 상호 정보를 공유하는 시점에 IP선점이라는 취약점이 발생하는데, 일반적인 네트워크 인프라에 방화벽 또는 웹 방화벽과 같은 L3 계층의 장비가 단독으로 구성 시에는 보안정책에 의거 적용되어진 IP에 대한 접근과 허용이 바로 네트워크 접근 경로에 적용되지만, L2 계층의 장비가 L3 장비가 이미 구현되어진 네트워크에 추가 적용되는 시점에는 L2 계층과 L3 계층을 대상으로 하는 장비 간에 보안정책 적용 시점에 시간적인 공백이 발생함으로써 공격의 포인트가 노출되어 진다. 따라서 내부 네트워크를 구현하고 L2 장비의 정책적용부터 L3 장비의 최종 보안정책 구현까지의 단계별 구성과 변화를 기술했다.

2.1. 내부 네트워크 구성

본 연구에서는 TCP/IP Layer의 L2 계층 장비를 신규로 기존 네트워크 인프라에 구현하는 1단계 인프라 조정과 L3 계층의 정보보안 장비를 구현하는 2단계 인프라 조정을 전제조건으로 한다. 2단계는 L3 계층의 정보보안 장비인 Firewall과 Web-Firewall을 순차적으로 추가 구현함으로써 발생하는 취약점을 실험하고 분석결과에 따른 방어방법을 제안한다. 취약점 분석을 위한 첫 번째 구성은 Firewall의 특정 IP 영역 정책설정과 IP 선점(Preoccupation), 두 번째는 Firewall과 Web-Firewall에 동시에 동일한 특정 IP 영역 정책설정을 실험한다. 또한, Firewall 장비는 제한된 Port구성으로 3개만을 운영한다. Port-No 1은 Internal Network Area에 연결되고 Port-No 2는 Firewall Management System에 하고 마지막 Port-No 3은 Firewall 정책에서 그림 1과 같이 가상으로 구현함으로써 Firewall Traffic을 Load-Balancing이 가능하도록 최적 자원 환경으로 구현한다. 또한, Web-Firewall 역시 제한된 Port구성으로 2개만을 운영한다. 그림 2와 같이 Port-No 1은 Switch에 연결되고 Port-No 2는 Web-server에 연결한다[1][2][3].

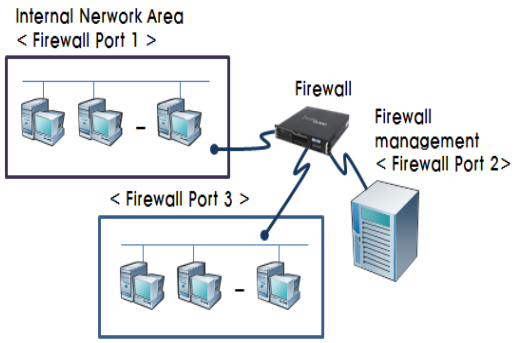

그림 1. Firewall Port 구성과 네트워크 인프라 구현
Fig. 1 Firewall Port Composition & Infrastructure Design

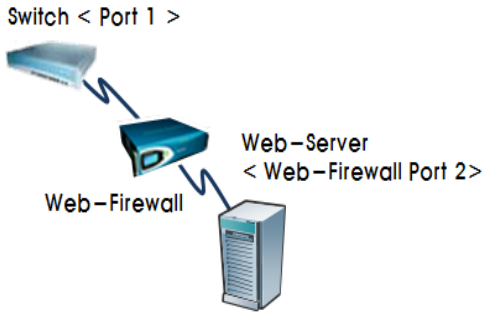

그림 2. Web-Firewall Port 구성과 네트워크 인프라 구현
Fig. 2 Web-Firewall Port Composition & Network Infrastructure Design

2.2. L2 계층 Switching 운영

과거 L2 장비의 경우는 가장 많은 기능 중에서 단순 Switching 기능만을 구현하기 위해 운영되어졌다. 서로 다른 내부 네트워크 가상 기반을 구현하기 위해 Virtual-mode Switching으로 구현되어 지기도 했지만, 대역폭 감소로 인한 전송속도의 저하 등 다양한 문제점이 있어서 L3 계층의 Routing 기능은 접목되어지지 않았다. 하지만 21세기 현재에는 L2 계층의 장비와 L3 계층의 장비가 상호 Switching 및 Routing 기능을 유기적으로 변형하여 사용할 수 있는 복합기능을 구현한다. 따라서 내부 네트워크 정보보안을 위한 인프라 관리자에게는 단순 연결과 별도의 Customizing이 없이도 설치와 운영이 가능하기 때문에 단순 하드웨어적인 연결만을 우선하고 L2 계층의 장비가 추가된 이후 발생 가능한 정책 적용을 위한 Latency Time 발생과 L3 계층의 정보보안 장비의 IP 선점(Preoccupation)으로 인한 보안 취약점을 확인하지 못한다[4].

2.3. Firewall 특정 IP 영역 정책 설정

L2 계층 하단에 Firewall 장비를 우선 연결하고 웹서버를 추가 연결한다. 또한, 웹서버 연결 이전에 Firewall에 특정 IP에 대역에 대한 접근제한에 대한 정책을 설정한다. 접근제한 정책 범위의 IP 대역은 그림 3과 같다. 웹서버 IP는 접근제한 IP 범위 내의 특정 IP를 부여한다.

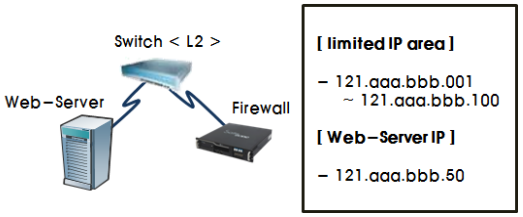

그림 3. 특정 IP에 대역에 대한 접근제한 정책 설정
Fig. 3 Establishment of Policies to Limit the Access to a Particular IP Band

2.4. Web-Firewall 특정 IP 관제정책 설정

1단계 실험을 위해 구성한 특정 IP에 대역에 대한 접근제한 정책 설정에 추가로 웹서버와 L2 계층 장비 사이에 Web-Firewall을 추가 연결한다. 또한, Web-Firewall에 특정 IP에 대역에 대한 관제정책을 설정한다. 관제정책 범위의 IP 대역은 그림 4와 같다. Web-Firewall IP는 동일한 L2 계층 장비에 연결되어 있는 Firewall의 접근제한 IP 범위 내의 특정 IP를 부여한다[5].

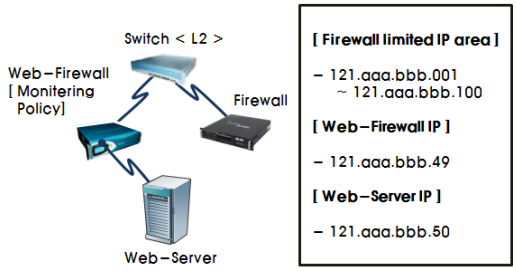

그림 4. 특정 IP에 대역에 대한 접근제한 정책 설정
Fig. 4 Establishment of Policies to Limit the Access to a Particular IP Band

2.5. IP 선점(Preoccupation)과 Latency Time분석을 통한 실험

1단계 Firewall 특정 IP 영역 정책 설정 이후 웹서버를 구축함으로써 웹서버의 정상적인 콘텐츠 제공이 인터넷 상에 이루어지는지에 대한 부분과 Firewall로 IP 선점(Preoccupation)이 이루어져서 웹서버가 차단되는 Latency Time을 확인한다. 또한, 2단계로 Web-Firewall의 특정 IP 관제정책 설정 이후 웹서버의 정상적인 콘텐츠 제공이 인터넷 상에 이루어지는지에 대한 부분과 Firewall로 IP 선점(Preoccupation)이 이루어져서 웹서버가 차단되는 Latency Time이 발생하는지에 대한 부분을 확인한다. 1, 2단계의 실험환경을 구성하고 순차적으로 실험을 구현한다[6].

III. 정보보안 장비의 특정 IP 영역 정책설정을 기반의 취약점 분석

3.1. Firewall의 IP 선점(Preoccupation)과 Latency Time 분석

1단계 실험 실행결과에 따라 IP 선점(Preoccupation) 결과, Latency Time 비율, Packet 트래픽 비율 등 결과를 분석한다. 네트워크 인프라를 구현하고 실험을 진행한 일반적인 결과로는 통신이 시작된 이후 일정간격 동안은 Latency Time 속도 저하 및 통신장애는 전혀 발생하지 않았으며. Packet 트래픽은 표 1과 같이 안정적인 In, Out, Drop Packet 비율을 나타냈다.

표 1. 네트워크 Packet Traffic 비율
Table 1. Network Packet Traffic Ratio

Port	Rate	bps	In-P	Out-P	Drop-P	In-B	Out-B	Drop-B
1	2 %	2,499 Kbps	341	545	0	18 KB	606 KB	0
2	0 %	45Kbps	76	106	0	4 KB	6 KB	0
3	2 %	2,503 Kbps	556	315	1	608 KB	17 KB	44

또한, 최종 인프라 구현 시에 Packet 전송 통신라인 테스트 명령인 “ping” 명령을 실행해도 그림 5와 같이 별다른 TTL(packet time-to-live) 저하는 발생하지 않는다. 하지만, 불규칙적인 시간 간격을 두고 통신이 두절되는 경우가 발생하고 보여 지는 정상적인 Latency Time 비율, Packet 트래픽 비율수치와는 무관하게 Firewall로 IP를 선점(Preoccupation) 당하고 통신이 차단된다.

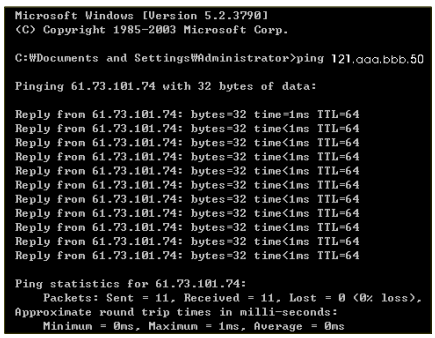

그림 5. “ping” 테스트와 TTL(packet time-to-live) 현황
Fig. 5 “Ping” Test & TTL (Packet Time-To-Live) Status

Firewall의 Port별 IP 선점(Preoccupation) 시점에 따른 변화는 그림 6과 같이 정상적인 Packet 흐름이 일정기간 유지되다가 IP를 선점(Preoccupation)하고 제한정책에 의해 웹서버로 접근하는 외부 통신로가 차단된다.

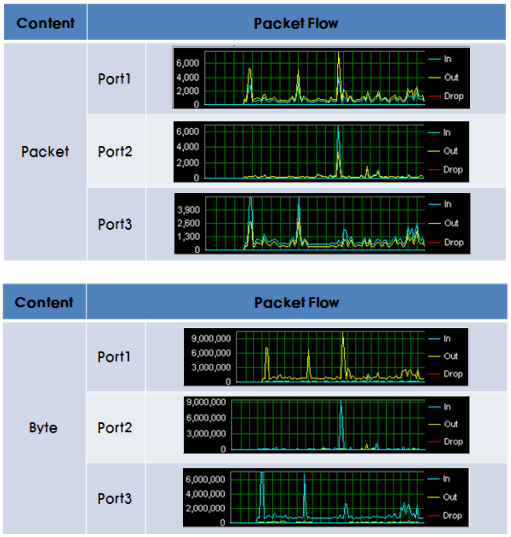

그림 6. Firewall Port Packet 분석
Fig. 6 Firewall Port Packet Analysis

3.2. Web-Firewall의 IP 선점(Preoccupation)과 Latency Time 분석

2단계 실험 실행결과에 따라 IP 선점(Preoccupation) 결과, Latency Time 비율, Packet 트래픽 비율 등을 1단계 실험결과와 같이 비교 분석한다. Web-Firewall이 L3 계층의 기능인 Routing 기능이 있음에도 불구하고 IP를 지속적으로 선점(Preoccupation)하지 못하고 1단계 실험과 같이 Firewall의 제한정책의 영향으로 통신이 차단된다. 또한, 최초 연결 시에 정상적인 Latency Time 비율, Packet 트래픽 비율수치를 보였다.

3.3. 적용 정책과 보안 취약점 분석 결과

L2 계층에 특정 목적의 서버를 운영하는 방법과 Firewall과 동등한 계층의 정보보안 장비를 설치 및 구현하는 방법을 적용함으로써 Firewall의 제한정책에 의해 IP를 선점(Preoccupation)이 이루어지

는 일정시간 동안 발생하는 Latency Time을 침해 공격이 가능하다. 두 가지 실험의 경우 표 2와 같이 동일한 공격 가능한 Latency Time이 존재함으로써 최종 Packet 흐름 비율은 2~5%의 결과가 나타났다.

표 2. 1, 2단계 실험결과 비교 분석
Table 2. Comparative Analysis on the 1st- & 2nd-step Experiment Results

Content	Latency Time	Packet Flow Rate	IP Preoccupation
Case 1	occurrence	Within 2 %	occurrence
Case 2	occurrence	Within 5 %	occurrence

기존에 구현되어 운영하던 네트워크 인프라의 경우는 L2 또는 L3 기반의 네트워크 장비가 확연히 구분되어 있어서 오히려 네트워크 인프라를 구현 시에 상이한 계층의 장비의 경우는 물리적인 통신 라인 연결에만 활용되어졌다. 따라서 L2 계층과 L3 계층의 확실한 장비간의 구분이 이루어져 있어서 IP를 선점하는 순간에 발생하는 취약점이 없었으나, 현재는 다양한 장비를 이미 구현한 이후 새롭게 네트워크 내에 추가 되어지는 L2 장비로 인한 취약점이 발생하는 것이다.

3.4. 취약점 보완과 방어기법 적용방향

Firewall의 제한정책 설정이 적용되는 시점인 IP 선점(Preoccupation)까지의 일시적인 공격 시간대가 발생하는 부분에 대해서 그림 7과 같이 L2 계층의 장비에 단순한 Switching과 Routing기능을 부가적으로 탑재해서 네트워크 인프라를 구축 시에는 공격자에게 Firewall에 설정한 정책과 무관하게 접근 가능한 취약점이 노출된다. 따라서, 반드시 TCP/IP Layer별 기능을 탑재한 L3 계층 이상의 보안장비의 보안 취약점을 해소하기 위해 네트워크 인프라 구현을 위한 가장 낮은 등급의 L2 장비를 제외하고 L2 계층의 기능까지 구현이 가능한 동등한 L3 계층 이상의 장비를 추가 구현해야 한다.

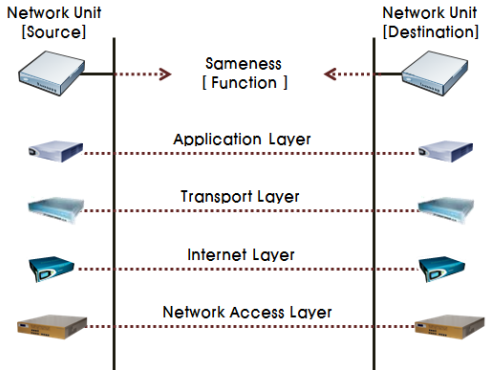

그림 7. TCP/IP Layer 등급별 장비 구성
Fig. 7 Equipment Composition by TCP/IP Layer Grade

IV. 결 론

본 논문에서는 가장 낮은 TCP/IP Layer의 통신정책을 구현하는 L2 계층기반의 Switching 운영 시에 보안 취약점을 언급을 했으며, 단순 Switching 장비 구현실험과 동등한 계층의 정보보안 장비 구현 실험을 통해서 불규칙적으로 최초 구축 이후 Latency Time을 두고 통신이 두절되며, Firewall의 제한정책 설정을 반영하는 문제에 대해서 Packet 흐름, 통신 비율, In, Out, Drop Packet 현황 등을 다양하게 검토 및 분석하였다. 최종 분석결과에 따른 결론으로는 TCP/IP Layer 통신정책 기반의 동등한 계층 간의 장비를 구현함으로써 Latency Time을 최소화할 수 있으며, L3 기반의 보안정책 구현 방법인 Routing 기능을 탑재함으로써 공격 가능한 취약점을 최소화 한다. 또한, IP 선점(Preoccupation), 접근 기능회수라고도 표현되는 보안 취약점을 최소화할 수 있다. 해당 IP 선점(Preoccupation)까지의 Latency Time이 지속적으로 발생하면, 중요 데이터베이스를 대상으로 실시간 처리를 하는 시스템과 서로 다른 이질적인 네트워크 구간에서의 Trust-membership 정책과 병렬 처리와 같은 시스템은 제3자의 시스템 침해로 인해 치명적인 장애를 얻을 수도 있다. 향후 네트워크 인프라 재 구현을 위한 솔루션 설계에는 반드시 TCP/IP Layer의 계층별 동등한 기능을 구현하는 장비를 기반으로 구성해야 하며, TCP/IP Layer 통

신정책을 모두 탑재하고 탑재된 정책대비 처리속도 비율이 비례하는 L2 장비의 기술적인 제안과 연구가 필요하다.

참고 문헌

[1] Wool .A, “Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese”, IEEE internet computing, V.14 No.4, pp.58-65, 2010.

[2] Li .F, Yu .N, "Design and Implementation of TCP/IP Protocol Learning Tool", Springer, pp.46-52, 2010.

[3] Harrison .R, "Firewall Management Today and Tomorrow", Database and network journal, V.40 No.4, pp.18-19, 2010.

[4] Li Xinlei, Zheng Kangfeng, Yang Yixian, "A DDoS attack defending scheme based on network processor", 2009 WASE International Conference on Information Engineering, pp.238-241, 2008.

[5] Rahul Kumar, Rahul Karanam, Rahul Chowdary Bobba, Raghunath .S, "DDOS DEFENCE MECHANISM", 2009 International Conference on Future Networks, pp.254-257, 2009.

[6] Zhen YE, Weiwei SHI, Dayong YE, "DDoS Defense Using TCP_IP Header Analysis and Proactive Tests", 2009 International Conference on Information Technology and Computer Science, pp.548-552, 2009.

저자 소개

서우석(Woo-seok Seo)

2006년 8월 숭실대학교 정보과학대학원 정보통신융합학과(공학석사)

2006년 4월~현재 서울특별시 용산구시설관리공단 근무

2009년 9월~현재 숭실대학교 일반대학원 컴퓨터학과 (박사과정)

※ 주관심분야 : 정보보호, 네트워크 보안, 방화벽, Network Design 등

전문석(Moon-seog Jun)

1981년 2월 숭실대학교 전자계산학과 졸업

1986년 2월 University of Maryland Computer Science 석사

1989년 2월 University of Maryland Computer Science 박사

1986년 9월~1989년 12월 University of Mary 강사

1989년 3월~7월 Morgan State University 조교수

1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원

1991년 3월~현재 숭실대학교 정교수

※ 관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학